10.3. Cable Management for Shared Government Facilities

Objective

10.3.1. Cable management systems in shared government facilities are implemented in a secure and easily inspectable and maintainable way.

Context

Scope

10.3.2. This section provides specific requirements for cabling installed in **shared** Government facilities.

- A **shared** facility is a facility occupied by **more than one** agency. A shared facility should have stricter physical and technical security controls than a non-shared facility.
- A **non-shared** facility is a facility occupied **solely** by a single agency.

10.3.3. This section is to be applied in addition to common requirements for cabling as outlined in the Section 10.1 - Cable Management Fundamentals.

Applicability of controls within this section

10.3.4. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside of New Zealand, Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual will need to be consulted.

Rationale & Controls

Use of fibre optic cabling

10.3.5.R.01. **Rationale**

Fibre optic cabling does not produce and is not influenced by electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects especially in a shared facility where you do not have total control over other areas of the facility.

10.3.5.R.02. **Rationale**

It is more difficult to tap than copper cabling.

10.3.5.R.03. **Rationale**

Many more fibres can be run per cable diameter than wired cables thereby reducing cable infrastructure costs.

10.3.5.R.04. **Rationale**

Fibre cable is the best method to future proof against unforeseen threats.

10.3.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2295]

Agencies SHOULD use fibre optic cabling.

Cabling inspection

10.3.6.R.01. **Rationale**

In a shared facility it is important that cabling systems are inspected for illicit tampering and damage on a regular basis and have stricter controls than a non-shared facility.

10.3.6.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2299]

In TOP SECRET areas, cables MUST be fully inspectable for their entire length.

10.3.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2298]

Cabling SHOULD be inspectable at a minimum of five-metre intervals.

Cables sharing a common reticulation system

10.3.7.R.01. **Rationale**

In a shared facility with another government agency, tighter controls may be required for sharing reticulation systems. Note also the red/black separation requirements in paragraph 10.1.5.

10.3.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2302]

Approved cable groups SHOULD have either a dividing partition or a visible gap between the individual cable groups. If the partition or gap exists, cable groups may share a common reticulation system.

Enclosed cable reticulation systems

10.3.8.R.01. **Rationale**

In a shared facility with another government agency, TOP SECRET cabling is enclosed in a sealed reticulation system to restrict access and control cable management.

10.3.8.C.01. **Control System Classifications(s): Top Secret; Compliance: Should** [CID:2305]

The front covers of conduits, ducts and cable trays in floors, ceilings and of associated fittings that contain TOP SECRET cabling, SHOULD be clear plastic.

Cabling in walls

10.3.9.R.01. **Rationale**

In a shared facility with another government agency, cabling run correctly in walls allows for neater installations while maintaining separation and inspectability requirements. Controls are slightly more stringent than in a non-shared facility.

10.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2308]

Cabling from cable trays to wall outlets SHOULD run in flexible or plastic conduit.

Wall penetrations

10.3.10.R.01. **Rationale**

Wall penetrations by cabling, requires the integrity of the classified area to be maintained. All cabling is encased in conduit with no gaps in the wall around the conduit. This prevents any visual access to the secure area.

10.3.10.C.01. **Control System Classifications(s): Top Secret; Compliance: Should** [CID:2311]

For wall penetrations that exit into a lower classified area, cabling SHOULD be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Power reticulation

10.3.11.R.01. **Rationale**

In a shared facility with lesser-classified systems, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means.

10.3.11.C.01. **Control System Classifications(s): Top Secret; Compliance: Should** [CID:2314]

TOP SECRET facilities SHOULD have a power distribution board, separately reticulated, located within the TOP SECRET area and supply UPS power to all equipment.

Power Filters

10.3.12.R.01. **Rationale**

Power filters are used to provide a filtered (clean) power supply and reduce opportunity for technical attacks. See also 10.1.32.

10.3.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2317]

Power filters SHOULD be used to provide a filtered power supply and reduce opportunity for technical attacks.

Cabinet separation

10.3.13.R.01. **Rationale**

Having a visible gap between cabinets facilitates inspection for any unauthorised, malicious or cross patch cabling.

10.3.13.C.01. **Control System Classifications(s): Top Secret; Compliance: Should** [CID:2320]

TOP SECRET cabinets SHOULD have a visible gap to separate them from lower classified cabinets.